UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/821,754	03/30/2001	Matthew N. Schmid	CIG-101	5170

28970 7590 08/24/2005

PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 TYSONS BOULEVARD
MCLEAN, VA 22102

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

47

Office Action Summary	**Application No.** 09/821,754	**Applicant(s)** SCHMID ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _07 June 2005_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _2-21_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _2-21_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 7 June 2005, with an original application filed 30 March 2001, with acknowledgement of a continuing data filing date of 31 March 2000.

2. Claim 2-21 are currently pending in this application. Claims 2, 12, and 20 are independent claims. Claims 2, 12, and 20 have been amended.

Response to Arguments

3. Applicant's arguments with respect to claims 2-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 2, 3, 4, 5, 6, 10, 12, 13, 14, 15, 17, 18, 19, 20, and 21** are rejected under 35 U.S.C. 102(e) as being anticipated by O'Brien et al. U.S. Patent No. 6,658,571 (hereinafter '571).

As to independent claim 2, "A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:" is taught in '571 col. 2, lines 11-19 (i.e. unauthorized user application is interpreted as a corrupt program);

"inserting into a kernel of the operating system a substitute process creation function" is shown in '571 col. 2, line 61 through col. 3, line 12 (the substitute process creation function is one task wrapping the applications in hypervisors in a security framework 101 provides by controlling access to resources and processes; therefore "a substitute process creation function" is one part of the "security framework" described in '571) ;

"intercepting a request for execution of an application executable by a user using the substitute process creation function" is disclosed in '571 is col. 2, lines 24-39 (part of the security framework is a security master which intercepts system calls, the system call is interpreted to have the same meaning as a request for execution of an application);

"communicating information about the request from the substitute process creation function to a user-mode application running as a service on the operating stem, wherein the communicating information about the request from the substitute process creation function to a user-mode application occurs within the operating system" is taught in '571 col. 3, line 34 through col. 4, line 13;

"comparing the information to a list of authorized executables for the user using the user-mode application" is taught in '571 col. 5, lines 1-46;

"if the information does not match an item on the list, communicating a first message to deny the request from the user-mode application to the substitute process

creation function; and if the information does match an item on the list, communicating a second message to permit the request from the user-mode application to the substitute process creation function" is shown in '571 col. 6, lines 5-34.

As to dependent claim 3, **"wherein the inserting into a kernel of the operating system a substitute process creation function comprises: creating a device driver; loading the device driver into the kernel;** is disclosed in '571 col. 2, line 61 through col. 3, lines 13 (It is interpreted that a "device driver" is layer of software between the hardware and the operating system.)

"and modifying a table consulted by a dispatcher using the device driver, wherein the modifying a table causes the dispatcher to call the substitute process creation function in place of a second process creation function" is taught in '571 col. 3, line 65 through col. 4, line 13.

As to dependent claim 4, **"wherein the loading the device driver comprises one of dynamically loading into the kernel and loading into the kernel as part of a boot sequence** is disclosed in '571 col. 9, lines 5-20 (It is inherent that the security framework described loads the hypervisors as part of a normal computer boot sequence).

As to dependent claim 5, **"wherein the substitute process creation function is a wrapper around a process creation function provided by the operating system"** is shown in '571 col. 2, lines 61-67.

As to dependent claim 6, **"wherein the process creation function provided by the operating system comprises ZWCreateProcess"** is disclosed in '571 col. 4, lines 5-13 (As part of the security framework, the Security manager provides an interface for the user, therefore new applications can be wrapped and created).

As to dependent claim 10, "wherein the comparing the information to a list comprises comparing an application executable name of the information with an application executable name of at least one item from the list" is taught in '571 col. 5, lines 1-46.

As to dependent claim 12, "wherein the communicating information about the request comprises one or more of releasing a semaphore, calling an application program interface function, polling, using a socket, and using a pipe" is disclosed in '571 col. 5, line 55 through col. 6, line 4.

As to dependent claim 13, "wherein the communicating a first message to deny the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe" is taught in '571 col. 6, lines 6-62.

As to dependent claim 14, wherein the communicating a second message to permit the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe" is shown in '571 col. 6, lines 6-62.

As to independent claim 15, "A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:" is taught in '571 col. 2, lines 11-19;

"inserting into a kernel of the operating system a substitute process creation function" is shown in '571 col. 2, line 61 through col. 3, line 12;

"intercepting a request for execution of an application executable by a user using the substitute process creation function" is disclosed in '571 is col. 2, lines 24-39;

"communicating information about the request from the substitute process creation function to a user-mode application running as a service on the operatin system, wherein the communicating information about the request from the substitute process creation function to a user-mode application occurs within the operating system" is taught in '571 col. 3, line 34 through col. 4, line 13;

"prompting the user for authorization to proceed using the user-mode application" is shown in '571 col. 5, lines 1-27 (prompting the user for authorization to proceed using the user-mode application is interpreted to have the same meaning as "Device 203 facilitates communication between user space and security master ... Device 203 allows user 113 to ... dynamically configure a security module 105 including updating the security policy")

"if the authorization is not provided, communicating a first message to deny the request from the user-mode application to the substitute process creation function; and if the authorization is provided, communicating a second message to permit the request from the user-mode application to the substitute process creation function" is shown in '571 col. 6, lines 5-34.

As to dependent claims 17-19, these claims are substantially similar to claims 3-5; therefore they are rejected along similar rationale.

As to independent claim 20, this claim is directed to a system of the method of claim 2; therefore it is rejected along similar rationale.

As to dependent claim 21, "further comprising an administrative server, wherein the administrative server is in communication with the user-mode application, and wherein the usermode application downloads the list from the administrative server" is taught in '571 col. 3, lines 13-25 and col. 5, lines 1-15.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 7, 8, 9, and 11,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '571 in further view of Shostack et al. U.S. Patent No. 6,298,445 (hereinafter '445) in further view of Gooderum et al. U.S. Patent No. 6,219,707 (hereinafter '707).

As to dependent claim 7, the following is not taught in '571 **"wherein the information comprises one or more of a user domain, an application executable name, and a cryptographic identifier of an application executable"** however '445 teaches "Additionally, the integration can also perform a check on the integrity and authenticity of the software enhancement provided. This feature determines whether the user being sent the software enhancement is eligible, and checks the integrity and authenticity of the software enhancement.

In determining the integrity and authenticity of the software enhancement, the push system can use digital signatures or other cryptographic techniques" in col. 8, lines 19-31.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '571 that teach a method for computer security with application wrapping to include a means to utilize cryptographic techniques. One of ordinary skill in the art would have been motivated to perform such a modification to protect a computer network from attack by malicious outsiders (see '445 col. 2, lines 18 et seq.). "Whenever an unauthorized user breaches network security and is allowed free access to the system, the damage that might result is unpredictable. However, because some of the system vulnerabilities and techniques used by hackers are known, a system administrator may use that information to make the network less vulnerable to attack. However, the system administrator is required to remain constantly vigilant as to the new attacks being used by hackers, and then use that information to protect the network, clients and servers from the newly found vulnerability".

As to dependent claim 8, **"wherein the cryptographic identifier of an application executable comprises a hash created using an MD5 cryptographic algorithm"** is shown in is taught in '445 col. 11, lines 17-31 "The message that is signed is typically a condensed version of the actual message produced by a message digest (MD) or hash algorithm. In general, a message digest algorithm, takes as an input a message of arbitrary length and produces a shorter fingerprint of the input. In the disclosed invention, the message digest algorithm used is called MD5 and produces a 128-bit fingerprint".

As to dependent claim 9, **"wherein the list comprises one or more of an application executable name and a cryptographic identifier of an application executable"** is shown in

‘445 col. 10, lines 21-60 “Prior to installing the software enhancement on a computer or on a local server 18, the authenticity and integrity of the software enhancement is determined. The authenticity checks may occur either at user’s computer or at the local server 18. The authenticity checks include performing a cryptographic technique by verifying the user before installing the software enhancement”

As to dependent claim 11. The method of claim 2, wherein the comparing the information to a list comprises comparing a cryptographic identifier of the information with a cryptographic identifier of at least one item from the list” is taught in ‘445 col. 10, lines 21-60.

8. **Claim 16** is rejected under 35 U.S.C. 103(a) as being unpatentable over ‘571 in further view of Gooderum et al. U.S. Patent No. 6,219,707 (hereinafter ’707).

As to dependent claim 16, the following is not taught in ‘571 “wherein the authorization comprises a password” however ‘707 teaches “The rest of the installation is HTML forms-driven through the browser. Various items such as port number for the Commerce server, UID to run the server under, install directory, logging, administration password, and other server configuration are entered via three forms” in col. 25, lines 10-15.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of ‘571 that teach a method for computer security with application wrapping to include a means to protect the kernel of the operating system. One of ordinary skill in the art would have been motivated to perform such a modification to protect a computer network from attack by malicious outsiders (see ‘707 col. 1, lines 23 et seq.). “To protect themselves from attacks by malicious outsiders, organizations are turning to mechanisms for increasing network security. One such mechanism is described in "SYSTEM AND METHOD FOR PROVIDING SECURE INTERNETWORK SERVICES", U.S. patent application Ser. No. 08/322,078 filed Oct. 12, 1994 by Boebert et al., the discussion of which is hereby incorporated by reference. Boebert teaches that modifications can be made to the kernel of the operating system in order to add type enforcement protections to the operating system kernel. This protection mechanism can be added to any other program by modifications to the program code made prior to compiling. It cannot, however, be used to add type enforcement protection to program code after that program code has been compiled".

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Freund	U.S. Patent No. 5,987,611	issued dated: Nov. 16, 1999
Epstein et al.	U.S. Patent No. 6,684,329	issued dated: Jan. 25, 2004

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 1:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
18 August 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100